UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/582,633	06/12/2006	Martin Naedele	1004501-000848	2009

21839 7590 10/02/2008
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
SQUIRES, BRETT S	
ART UNIT	PAPER NUMBER
2131	
NOTIFICATION DATE	DELIVERY MODE
10/02/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	**Application No.** 10/582,633	**Applicant(s)** NAEDELE ET AL.	
	Examiner BRETT SQUIRES	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 June 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *06/12/06*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Specification

1. The abstract of the disclosure is objected to because of the reference to "(Fig. 2)" on page 17 line 15. Correction is required. See MPEP § 608.01(b).

Claim Objections

2. Claims 1-10 are objected to for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1, 3, and 8 recite "and/or," this claim language causes ambiguity in determining what elements are required by the claims. The examiner respectfully points out that for examination purposes "and/or" is construed to mean or. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2, 6-7, and 10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 2 recites the improper Markush Group of "data sources comprise routers, firewalls, hosts, applications, switches, NIDS, HIDS, or any combination thereof." The use of "comprising," and "any combination thereof," when claiming a Markush Group is improper because "comprising," and "any combination thereof," allow for inclusion of additional unrecited elements, and therefore renders the Markush Group indefinite. Appropriate correction is required.

Claim 3 recites the improper Markush Group of “numerical values maintained via increment/decrement operations, rate calculations, pass-through of values or evaluation of mathematical expressions involving multiple values or any combination thereof, and/or textual values maintained via template matching, text transformation, text translation, and composition of text from templates, text strings from incoming data and numerical values from incoming data or any combination thereof.” The use of “comprising,” and “any combination thereof,” when claiming a Markush Group is improper because “comprising,” and “any combination thereof,” allow for inclusion of additional unrecited elements, and therefore renders the Markush Group indefinite. Appropriate correction is required.

Claim 6 recites the limitation "the displaying means" on page 3 line 20 of the preliminary amendment filed June 12, 2006. There is insufficient antecedent basis for this limitation in the claim. Appropriate correction is required.

Claim 7 recites the limitation "the displaying means" on page 3 line 26 of the preliminary amendment filed June 12, 2006. There is insufficient antecedent basis for this limitation in the claim. Appropriate correction is required.

Claim 10 recites the limitations "said status and trend presenting means," and “said countermeasures initiating means” on page 4 lines 18-20 of the preliminary amendment filed June 12, 2006. There is insufficient antecedent basis for these limitations in the claim. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-3, 5-6, and 8-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Nazzal (US 2004/0261030).

Nazzal discloses an anomaly detection system having data sources located on or constituting the network with means for generating network-security relevant data (“Network Devices” See fig. 2 ref. no. 15 and paragraphs 42-44), an input module with input handlers for various protocols to connect to the data sources ("Collectors" See figs. 1-2 ref. no. 12 and paragraphs 42-44), at least one data processing module connected to the input module for access to the data sources with means for translating the network-security relevant data into quantitative variable ("Aggregator" See figs. 1-2 ref. no. 14, paragraphs 44-46 and 52), a supervisory system with means for presenting processed data to a security system operator (“Graphic User Interface of the Operator Console” See fig. 1 ref. no. 16, fig. 29 ref. no. 300, paragraph 42, and paragraph 193), and an interface module with means for transferring the quantitative variable from the processing module to the supervisory system ("Operator Console" See fig. 1 ref. no. 16 and paragraph 42).

Regarding Claim 2:

Nazzal discloses the network devices are switches, hosts, routers, SPAN ports, or other passive link taps (See paragraph 42).

Regarding Claim 3:

Nazzal discloses the network-security relevant data is current bytes/second, packet/second, connections/hour, as well as other statistics (See paragraph 45).

Regarding Claim 5:

Nazzal discloses the aggregator receives reports from collectors and groups of collectors (See paragraphs 43-44).

Regarding Claim 6:

Nazzal discloses the graphic user interface of the operator console displays status information as quantitative trend graphs with historical data storage and zoom in/out function (See fig. 29 ref. no. 300).

Regarding Claim 8:

Nazzal discloses event severity is coded by a color or other indicia (See paragraph 196).

Regarding Claim 9:

Nazzal discloses aggregator stores historical data for anomaly detection system for comparison to current data for the anomaly detection system (See paragraph 45).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 4 is rejected under 35 U.S.C. 103(a) as being obvious over Nazzal (US 2004/0261030) in view of Symantec Antivirus for Macintosh copyright 1994.

Nazzal discloses the above stated anomaly detection system having means for displaying the variables to a system operator ("Graphic User Interface of the Operator Console" See fig. 1 ref. no. 16, fig. 29 ref. no. 300, paragraph 42, and paragraph 193).

Nazzal does not disclose the graphic user interface of the operator console has reaction facilities with means for initiating predefined countermeasures.

Symantec discloses responding to a suspicious activity by presenting the user with an alert box having a description of the suspicious activity, an allow option, a deny option, and a remember option (See pages 4-9 and 4-10).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the anomaly detection system disclosed by Nazzal to include operator based responses to a suspicious activity such as that taught by Symantec in order to prevent the anomaly detection system from automatically responding legitimate activities that are reported as suspicious activities (See Symantec page 4-9).

8. Claim 7 is rejected under 35 U.S.C. 103(a) as being obvious over Nazzal (US 2004/0261030) in view of Bhattacharya (US 2005/0060562).

Nazzal discloses the above stated anomaly detection system having means for displaying status information ("Graphic User Interface of the Operator Console" See fig. 1 ref. no. 16, fig. 29 ref. no. 300, paragraph 42, and paragraph 193).

Nazzal does not disclose displaying a schematical depiction of the network and device structure and topology.

Bhattacharya discloses a system for displaying network security incidents that displays a schematical depiction of the network and device structure and topology (See figs. 4a-4b and 5a-5b).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include in the graphic user interface of the operator console disclosed by Nazzal a schematical depiction of the network and device structure and topology such as that disclosed by Bhattacharya in order to provide the operator with an overview of the scope of the network (See Bhattacharya paragraph 44).

9. Claim 10 is rejected under 35 U.S.C. 103(a) as being obvious over Rangachari (US 2003/017694) in view of Nazzal (US 2004/0261030) in further view of Symantec Antivirus for Macintosh copyright 1994.

Rangachari discloses an automation system for semiconductor fabrication having means for controlling the process of the automation system over the network ("Computer System having Multiple GUIs" See fig. 6 ref. nos. 502, 521, and paragraphs 54-55), the controlling means includes a human machine interface ("Multiple GUIs" See fig. 6 ref. no. 502 and paragraphs 54-55) with means for displaying information about the automation system to an automation system operator ("The GUI also provides a display of the equipment specific and process specific data." See paragraph 55) and means for entering commands for controlling the automation system ("The GUI also provides additional functions including an operator interface for the automation system for displaying the computer program related information; a manual operation mode for the SMIF input-output, including load, unload, read, Auto-ID device, initialize Auto-ID device, home, etc." See paragraph 55).

Rangachari does not disclose the automation system operator workstation is connected to a security system with the supervisory system is integrated into the automation system controlling means, the status and trend presenting means being included in the information displaying system of the human machine interface and the countermeasures initiating means being integrated in the commands entering means.

Nazzal discloses the above stated anomaly detection system having a supervisory system with means for presenting processed data to a security system operator ("Graphic User Interface of the Operator Console" See fig. 1 ref. no. 16, fig. 29 ref. no. 302, paragraph 42, and paragraph 193) and a status and trend presenting means (See fig. 29 ref. no. 300).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include in the automation system for semiconductor fabrication disclosed by Rangachari the anomaly detection system taught by Nazzal in order to provide the system operator with early detection of network attacks and security violations (See Nazzal paragraph 3).

Symantec discloses responding to a suspicious activity by presenting the user with an alert box having a description of the suspicious activity, an allow option, a deny option, and a remember option (See pages 4-9 and 4-10).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the above stated combination of the automation system for semiconductor fabrication disclosed by Rangachari and the anomaly detection system disclosed by Nazzal to include operator based responses to a suspicious activity such as that taught by Symantec in order to prevent the anomaly detection system from automatically responding legitimate activities that are reported as suspicious activities (See Symantec page 4-9).

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRETT SQUIRES whose telephone number is (571) 272-8021. The examiner can normally be reached on 9:00am - 5:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BS/

/Christopher A. Revak/
Primary Examiner, Art Unit 2131